Implicitizing rational curves by the method of moving quadrics

Laurent Busé

Université Côte d'Azur, Inria.

Clément Laroche

University of Athens, ATHENA Research and Innovation Center.

Fatmanur Yıldırım

Université Côte d'Azur, Inria.

Abstract

A new technique for finding implicit matrix-based representations of rational curves in arbitrary dimension is introduced. It relies on the use of moving quadrics following curve parameterizations, providing a high-order extension of the implicit matrix representations built from their linear counterparts, the moving planes. The matrices we obtain offer new, more compact, implicit representations of rational curves. Their entries are filled by linear and quadratic forms in the space variables and their ranks drop exactly on the curve. Typically, for a general rational curve of degree d we obtain a matrix whose size is half of the size of the corresponding matrix obtained with the moving planes method. We illustrate the advantages of these new matrices with some examples, including the computation of the singularities of a rational curve.

Keywords: parametrized curve, implicitization, μ-basis, moving quadric.

1. Introduction

Rational algebraic curves are widely and intensively used in Computer Aided Geometric Design. Their parametric representations are very useful at the design step because their control points allow to shape them intuitively. They are also very convenient for generating points along the curve, which is useful in many algorithms, such as rendering algorithms for instance. On the other hand, implicit representations are particularly interesting for determining whether a point lies on the curve, and more generally for dealing with intersection problems. Thus, both the parametric and the implicit representations of a rational curve are valuable in geometric modeling and there is an extensive literature on the implicitization problem, that is to say on the determination of an implicit representation of a curve from a parametric representation.

The implicitization of rational plane curves have been extensively studied. The method of moving lines introduced by Sederberg and Chen in 1995 [1], and then extended further three years later in the foundational paper [2] with the additional concept of μ-basis, gave a powerful solution to this problem. Indeed, not only this method allows to compute an implicit equation of the curve via the determinant of a non-singular matrix, but this matrix actually provides a much more interesting implicit representation of the curve. First, the matrix itself, without computing its determinant, can be used for determining if a point lies on the curve simply by evaluating its rank at this point. Second, if a point is detected on the curve, then its parameter(s) can be determined from the kernel of this matrix, whereas this is impossible to do with an implicit polynomial equation of the curve.

A μ-basis of a plane rational curve is composed of two polynomial equations that both define a line in the plane that moves when the parameter of the curve moves. As shown in [2], the matrix of moving lines can be interpreted as the classical Sylvester matrix of a μ-basis. Thus, if one starts from a degree d parameterization, this matrix a $d \times d$-matrix and its entries are linear polynomials in the plane coordinates. In order to obtain more compact matrices, but still with similar properties, one can consider the well-known (hybrid) Bézout resultant matrices of the μ-basis [3]. In this way, for a general curve defined by a parameterization of degree d, we obtain a square matrix of about half-size in comparison to the matrix of moving lines, but now some of the entries of this matrix are quadratic polynomials, instead of being all linear polynomials in the implicit variables. This approach for obtaining such more compact implicitization matrices with some quadratic entries is known as the method of moving conics. It has been introduced in [3] and then extensively used, especially to deal with the implicitization of rational surfaces (see e.g. [4, 5]).

Unlike the case of plane curves, the implicitization of parameterized curves in higher dimension is much more delicate because now the space curve is the intersection of several hypersurfaces. For instance, even determining the minimal number of such hypersurfaces is a difficult problem that has attracted a lot of attention from the algebraic geometers. On the contrary, the concept of μ-basis is easily generalized to curves in higher dimension [6, 7] and many

*Corresponding author

Email addresses: laurent.buse@inria.fr (Laurent Busé), claroche@di.uoa.gr (Clément Laroche), fatma.yildirim@inria.fr (Fatmanur Yıldırım)

results to produce some implicit polynomial equations of a curve from them have been proposed. However, the existing results provide only partial answers to this question and apply only in particular cases (see e.g. [8, 9, 10]).

In order to avoid this problem, another direction has been proposed in [11, 12]. It consists in using the elimination matrix built from a μ-basis as an implicit representation. Thus, this matrix of moving hyperplanes is the natural generalization of the Sylvester matrix of a μ-basis in the case of plane curves. Although this matrix is no longer a square matrix, it still allows to characterize the point that lie on the curve by a drop of its rank. In [11], the construction and the properties of this matrix has been studied, and it is shown how it allows to simplify intersection problems. In this paper, we develop further this approach. As already mentioned, in the case of plane curves the method of moving conics [3], based on the hybrid Bézout matrix of the μ-basis, is an important improvement as it allows to produce a more compact matrix compared to the Sylvester matrix of the μ-basis. The main contribution of this paper is a generalization of this method to the case of space curves, that we call the method of moving quadrics after [3]. In other words, we introduce a generalization to parameterized space curves of the hybrid Bézout matrix of a μ-basis. As in the case of plane curves, we will show that the gain in the size of the matrix is similar: for a general parameterized space curve, the size of the matrix of moving quadrics is about half of the size of the matrix of moving hyperplanes.

The paper is organized as follows. In Section 2 we revisit the method of moving conics [3] with a particular focus on Sylvester forms, a construction that is central in this paper. Then, in Section 3 we deal with the general case of parameterized curves in arbitrary dimension and state our main results. Their proofs use specific tools from algebraic geometry and commutative algebra; they have been concentrated in §3.4 so that a reader who is not familiar with these tools can easily skip it in a first reading. Finally, in Section 4 the effective computation of our new matrices is discussed and illustrated with some experiments. In particular, we illustrate the gain we obtain for the inversion of a point on the curve.

2. The method of moving conics

The implicitization of rational plane curves, that is to say the finding on an implicit equation of a plane curve from a parameterization, has been extensively studied in the past. Besides the basic method based on a resultant computation directly from a parameterization, the method of moving lines introduced by Sederberg and Chen in [1], and developed further with the concept of μ-basis in [2], has been the more powerful and fruitful one in geometric modeling. In this section, we briefly review it with a particular emphasis on its generalization to moving conics [3] that allows to obtain more compact matrices. Although there is no new result in this section, we believe that it sheds new light on this topic.

In what follows, we suppose that an homogeneous parameterization of a rational plane curve $\mathcal{C}$ is given over a field $\mathbb{K}$ by

$$\begin{array}{rccl} \phi: & \mathbb{P}^1 & \to \mathbb{P}^2 & \\ & (s:t) & \mapsto (f_0(s,t):f_1(s,t):f_2(s,t)), & \end{array} \tag{1}$$

where f_0, f_1 and f_2 are homogeneous polynomials in $\mathbb{K}[s,t]$ of the same degree $d \geqslant 1$. For the sake of simplicity, we assume that these polynomials have no common factor, so that the map ϕ is well defined everywhere on $\mathbb{P}^1$.

2.1. Moving lines

A *moving line* of degree $\nu \in \mathbb{N}$ is a polynomial of the form

$$L(s,t;x_0,x_1,x_2) = g_0(s,t)x_0 + g_1(s,t)x_1 + g_2(s,t)x_2$$

where g_0, g_1 and g_2 are homogeneous polynomials in $\mathbb{K}[s,t]$ of degree ν. For any point $(s_0:t_0) \in \mathbb{P}^1$, $L(s_0,t_0;x_0,x_1,x_2)$ is a linear form in the variables x_0,x_1,x_2 that can be interpreted as the defining equation of a line in $\mathbb{P}^2$. This line moves when the point $(s_0:t_0)$ varies in $\mathbb{P}^1$, hence its name. In addition, the moving line L is said to follow the parameterization ϕ if

$$L(s,t;f_0(s,t),f_1(s,t),f_2(s,t)) = g_0f_0 + g_1f_1 + g_2f_2 = 0.$$

Geometrically, this implies that the line defined in the plane by the equation $L=0$ goes through the point $\phi(s:t) \in \mathcal{C}$.

For any integer $\nu \geqslant 0$, it is straightforward to compute a basis $L_1,\dots,L_{r_\nu}$ of the vector space of moving lines of degree ν following ϕ by solving a simple linear system. We define the matrix $\mathbb{M}_\nu(\phi)$, or simply $\mathbb{M}_\nu$, as the matrix whose columns are filled with the coefficients of the moving lines L_j with respect to the variables s,t. More precisely, $\mathbb{M}_\nu$ is defined by the matrix equality

$$(L_1\ L_2\ \cdots\ L_{r_\nu}) = (s^\nu\ s^{\nu-1}t\ \cdots\ t^\nu)\cdot \mathbb{M}_\nu. \tag{2}$$

It is of size $(\nu+1)\times r_\nu$ and its entries are linear forms in $\mathbb{K}[x_0,x_1,x_2]$. Therefore, it has sense to evaluate the matrix $\mathbb{M}_\nu$ at a point $p \in \mathbb{P}^2$, which we denote by $\mathbb{M}_\nu(p)$.

Proposition 1. *For all integer $\nu \geqslant d-1$ we have $r_\nu \geqslant \nu+1$ and*

$$\operatorname{rank}\mathbb{M}_\nu(p) < \nu+1 \iff p \in \mathcal{C}.$$

In addition, $r_{d-1} = d$ and $r_\nu > \nu+1$ if $\nu \geqslant d$.

Proof. See [1] and [13, §2]. □

Thus, Proposition 1 shows that the matrices $\mathbb{M}_\nu$ are implicit representations of the curve $\mathcal{C}$ for all $\nu \geqslant d-1$, in the sense that they allow to discriminate the points $p \in \mathbb{P}^2$ that belong to the curve $\mathcal{C}$. Introduced first in [1] as the method of moving lines, the matrix $\mathbb{M}_{d-1}$ is a particular member in the family of matrices $\mathbb{M}_\nu$, $\nu \geqslant d-1$: it is a square matrix whose determinant gives an implicit equation of the curve $\mathcal{C}$ raised to the power the degree of ϕ [2, 13]. By the degree of ϕ we mean the number of pre-images of a general point on $\mathcal{C}$ via ϕ and over the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. In other words, this is nothing but the number of times the curve $\mathcal{C}$ is traced by the parameterization ϕ over $\overline{\mathbb{K}}$.

2.2. μ-basis

In the foundational paper [2], among other results the authors show that the matrices $\mathbb{M}_\nu$ exhibit a specific structure by introducing the concept of μ-basis.

Proposition 2. *There exists two moving lines p_1 and p_2 following ϕ such that any moving line L following ϕ can be written as*

$$L = h_1 p_1 + h_2 p_2,$$

where h_1 and h_2 are homogeneous polynomials in $\mathbb{K}[s,t]$. Such a couple of moving lines p_1, p_2 is a called a μ-basis of the parameterization ϕ.

In addition, the degrees μ_1 and μ_2 of the moving lines p_1 and p_2 only depend on ϕ and are such that $\mu_1 + \mu_2 = d$.

Proof. See for instance [2, 14]. □

As a consequence of this proposition, the vector space of moving lines we used to define the matrices $\mathbb{M}_\nu(\phi)$ have a simple description. More precisely, for any integer ν we have

$$\langle L_1, \dots, L_{r_\nu} \rangle = \\ \langle s^{\nu-\mu_1} p_1, s^{\nu-\mu_1-1} t p_1, \dots, t^{\nu-\mu_1} p_1, s^{\nu-\mu_2} p_2, \dots, t^{\nu-\mu_2} p_2 \rangle$$

where it is understood that the multiples of p_1, respectively p_2, disappear if $\nu < \mu_1$, respectively $\nu < \mu_2$. It follows that

$$r_\nu = \max(0, \nu - \mu_1 + 1) + \max(0, \nu - \mu_2 + 1).$$

Moreover, written in these special bases the matrices $\mathbb{M}_\nu$ exhibit a Sylvester-like block structure. In particular, in these bases the matrix $\mathbb{M}_{d-1}$ is nothing but the classical Sylvester matrix associated to the polynomials p_1 and p_2 with respect to the homogeneous variables s, t, denoted $\mathrm{Syl}(p_1, p_2)$. Thus, we recover the property that the resultant of these two polynomials, which is defined as the determinant of $\mathrm{Syl}(p_1, p_2)$, is equal to an implicit equation of $\mathcal{C}$ raised to the power the degree of ϕ.

Several methods have been proposed to compute a μ-basis. The first type of methods starts from a generating collection of moving lines following ϕ, namely the obvious moving lines of degree d of the form

$$f_i(s,t)x_j - f_j(s,t)x_i, \quad 0 \leqslant i < j \leqslant 2, \tag{3}$$

and uses various reductions to reach iteratively a μ-basis by means of linear algebra algorithms; see e.g. [14, 15]. Another type of methods arise from the computation of normal forms of matrices over a principal ideal domain, typically the computation of a Popov form; see e.g. [16, 17]. So far, these latter methods exhibit the best theoretical complexity.

The matrix $\mathbb{M}_{d-1}$ is the smallest matrix that is an implicit representation of the curve in the family of matrices $\mathbb{M}_\nu$. For a general parameterization ϕ, the implicit equation of the curve is a degree d homogeneous polynomial equation in $\mathbb{K}[x_0, x_1, x_2]$. Therefore, the matrices $\mathbb{M}_\nu$ with $\nu \leqslant d-2$ cannot yield an implicit representation of $\mathcal{C}$ because their entries are linear forms in $\mathbb{K}[x_0, x_1, x_2]$. As a consequence, to obtain more compact matrices it is necessary to introduce high-order extensions of the moving lines. Having in mind the correspondence between $\mathbb{M}_{d-1}$ and the Sylvester matrix $\mathrm{Syl}(p_1, p_2)$, the well-know family of (hybrid) Bézout matrices of p_1, p_2, which provides more compact matrices for the resultant, suggests to introduce quadratic forms in some entries of the matrices we consider.

2.3. Moving conics

As we call a moving line an equation of a line in the plane that moves as the parameter $(s : t) \in \mathbb{P}^1$ varies, we call a *moving conic* an equation of a conic in the plane whose coefficients depend on the parameter $(s : t) \in \mathbb{P}^1$. More concretely, a *moving conic* of degree $\nu \in \mathbb{N}$ is a polynomial of the form

$$Q(s,t;x_0,x_1,x_2) = g_{0,0}(s,t)x_0^2 + g_{0,1}(s,t)x_0x_1 + \\ g_{0,2}(s,t)x_0x_2 + g_{1,1}(s,t)x_1^2 + g_{1,2}(s,t)x_1x_2 + g_{2,2}(s,t)x_2^2$$

where the polynomials $g_{i,j}(s,t)$ are homogeneous polynomials of degree ν in $\mathbb{K}[s,t]$. In addition, this moving conic is said to follow the parameterization ϕ if

$$Q(s,t;f_0,f_1,f_2) = \sum_{0 \leqslant i \leqslant j \leqslant 2} g_{i,j}(s,t) f_i(s,t) f_j(s,t) = 0.$$

Similarly to moving lines, this latter condition means geometrically that the conic defined in the plane by the polynomial Q goes through the point $\phi(s : t) \in \mathcal{C}$.

We can consider the vector space of moving conics following the parameterization ϕ of degree ν and, similarly to what we did with moving lines, build a coefficient matrix from them. However, such a matrix is useless in general because its entries are exclusively quadratic forms in $\mathbb{K}[x_0, x_1, x_2]$ and hence the determinants of its minors are always polynomials of even degree. Having in mind the (hybrid) Bézout matrix that we previously mentioned, a better option is to combine both moving lines and moving conics in a same coefficient matrix. We proceed as follows.

Pick an integer $\nu \geqslant 0$. As explained in §2.1, choosing a basis of the vector space of moving lines following ϕ of degree ν, denoted $\langle L_1, \dots, L_{r_\nu} \rangle$, one can build the matrix $\mathbb{M}_\nu$. Now, one can consider the vector space W_ν of moving conics following ϕ of degree ν. As it turns out, each moving lines L_j gives the three moving conics x_0L_j, x_1L_j and x_2L_j that all follow the parameterization ϕ. Therefore, these $3r_\nu$ moving conics obtained from the moving lines, generate a sub-vector space V_ν of W_ν. By solving a linear system and computing a nullspace, one can compute a basis of the quotient vector space W_ν / V_ν that we denote by $\langle Q_1, \dots, Q_{c_\nu} \rangle$. Then, we define the matrix $\mathbb{MQ}_\nu(\phi)$, or simply $\mathbb{MQ}_\nu$, as the matrix satisfying to the equality

$$(L_1 \ L_2 \ \cdots \ L_{r_\nu} \ Q_1 \ \cdots \ Q_{c_\nu}) = (s^\nu \ s^{\nu-1}t \ \cdots \ t^\nu) \cdot \mathbb{MQ}_\nu. \tag{4}$$

It is a matrix of size $(\nu+1) \times (r_\nu + c_\nu)$. By definition, its first r_ν columns is simply the matrix $\mathbb{M}_\nu$ whose entries are linear forms in $\mathbb{K}[x_0, x_1, x_2]$, and its last c_ν columns are built from moving conics, so its entries are quadratic forms in $\mathbb{K}[x_0, x_1, x_2]$.

We recall that μ_1 and μ_2 denote the degrees of a μ-basis of ϕ. Without loss of generality we assume that $\mu_1 \leqslant \mu_2$.

Proposition 3. *If $\nu \geqslant \mu_2 - 1$ then $r_\nu + c_\nu \geqslant \nu + 1$ and*

$$\operatorname{rank} \mathbb{MQ}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

In addition,

- *if $\mu_2 - 1 \leqslant \nu \leqslant d-1$ then $r_\nu = 2(\nu+1) - d$, $c_\nu = d - 1 - \nu$ and the matrix $\mathbb{MQ}_\nu$ is a square matrix whose determinant is an implicit equation of $\mathcal{C}$, raised to the power the degree of ϕ,*

- *if $\nu \geqslant d-1$ then $c_\nu = 0$ and $\mathcal{MQ}_\nu = \mathcal{M}_\nu$.*

Proof. These results will be obtained in the next section §2.4 by interpreting the matrices $\mathcal{MQ}_\nu$ as resultant matrices. See also [3]. □

In the case where $\mu_1 = \mu_2 = k$, hence $d = 2k$, the matrix $\mathcal{MQ}_{k-1}$ is a $k \times k$-matrix whose entries are all quadratic forms, and whose determinant is an implicit equation of $\mathcal{C}$, raised to the power the degree of ϕ. This is the only setting where such a fully quadratic matrix appears in the family of matrices of moving lines and conics. Notice that a general curve ϕ such that $d = 2k$ satisfies to $\mu_1 = \mu_2$.

2.4. Sylvester forms

We already mentioned that the definition of the family of matrices $\mathcal{MQ}_\nu$ is inspired by the more classical family of (hybrid) Bézout matrices of a μ-basis p_1, p_2 of ϕ. In what follows, we make explicit this comparison and exhibit in the same time a structure for the matrices $\mathcal{MQ}_\nu$. For that purpose we need to introduce the Sylvester forms.

Let p_1, p_2 be a μ-basis of the parameterization ϕ and denote by $\mu_1 \leqslant \mu_2$ their respective degrees. We recall that $\mu_1 + \mu_2 = d$. Let $\alpha := (\alpha_1, \alpha_2)$ be any couple of non-negative integers such $|\alpha| := \alpha_1 + \alpha_2 \leqslant \mu_1 - 1$. Since p_1 and p_2 are homogeneous polynomials in the variables s, t, one can decompose them as

$$p_1 = s^{\alpha_1+1} h_{1,1} + t^{\alpha_2+1} h_{1,2},$$
$$p_2 = s^{\alpha_1+1} h_{2,1} + t^{\alpha_2+1} h_{2,2},$$

where $h_{i,j}(s, t; x_0, x_1, x_2)$ are homogeneous polynomials of degree $\mu_i - \alpha_j - 1$ with respect to the variables s, t and linear forms with respect to the variables x_0, x_1, x_2. Then, we define the polynomial

$$\mathrm{syl}_\alpha(p_1, p_2) := \det \begin{pmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{pmatrix}$$

and call it a *Sylvester form* of p_1, p_2.

Lemma 4. *For any α such that $|\alpha| \leqslant \mu_1 - 1$, the Sylvester form $\mathrm{syl}_\alpha(p_1, p_2)$ is a moving conic of degree $d - 2 - |\alpha|$ following the parameterization ϕ. Moreover, it is independent of the choice of the polynomials $h_{i,j}$ modulo the μ-basis p_1, p_2, equivalently modulo the vector space of moving conics $V_{d-2-|\alpha|}$ defined in §2.3.*

Proof. The first assertion follows by construction and by the Cramer's rules for solving a linear system; we refer to [18, §3.10] for more details. □

It turns out that the Sylvester forms generate all the moving conics following ϕ of degree greater or equal to $\mu_2 - 1$. Taking again the notation of §2.3, here is the precise result.

Proposition 5. *Let ν be an integer such that $\mu_2 - 1 \leqslant \nu \leqslant d - 2$. Then the set of $d - 1 - \nu$ Sylvester forms*

$$\{\mathrm{syl}_\alpha(p_1, p_2)\}_{|\alpha|=d-2-\nu} = \left\{\mathrm{syl}_{(d-2-\nu,0)}(p_1, p_2), \ldots, \mathrm{syl}_{(0,d-2-\nu)}(p_1, p_2)\right\}$$

form a basis of the quotient vector space W_ν / V_ν of moving conics of degree ν following ϕ and not generated from their corresponding moving lines, so that we have $c_\nu = d - 1 - \nu$. In addition, $W_{d-1} = V_{d-1}$ and hence $c_{d-1} = 0$.

Proof. These results follows from a duality property; we refer the reader to §2.1 and Theorem 2.9 in [19], and the references therein. See also §3.4. □

As a consequence of this proposition, the construction of the matrices $\mathcal{MQ}_\nu$, $\nu \geqslant \mu_2 - 1$, following (2) can be done with more specific choices of the bases of moving lines and moving conics of degree ν. As we already used in §2.2, the space of moving lines can be chosen such that

$$\langle L_1, \ldots L_{r_\nu} \rangle = \langle s^{\nu-\mu_1} p_1, s^{\nu-\mu_1-1} t p_1, \ldots, t^{\nu-\mu_1} p_1, s^{\nu-\mu_2} p_2, \ldots, t^{\nu-\mu_2} p_2 \rangle.$$

Moreover, by Proposition 5 the space of moving conics can be chosen as

$$\langle Q_1, \ldots Q_{c_\nu} \rangle = \langle \mathrm{syl}_{(d-2-\nu,0)}(p_1, p_2), \mathrm{syl}_{(d-3-\nu,1)}(p_1, p_2), \ldots, \mathrm{syl}_{(0,d-2-\nu)}(p_1, p_2) \rangle.$$

In this way, the matrix $\mathcal{MQ}_\nu$, $\nu \geqslant \mu_2 - 1$, exhibits a very particular structure: its first block of $r_\nu = 2(\nu+1) - d$ columns is the matrix $\mathcal{M}_\nu$, which is a Sylvester block built from the μ-basis p_1, p_2, and each of its last $c_\nu = d - 1 - \nu$ columns are filled with Sylvester forms of p_1 and p_2. This interpretation of the matrices $\mathcal{MQ}_\nu$, $\nu \geqslant \mu_2 - 1$, allows us to identify them with the family of (hybrid) Bézout matrices that are precisely defined in this way in the literature (see e.g. [20, 3]). The determinant of these Bézout matrices is known to be equal to the resultant of the μ-basis p_1, p_2. Therefore, we obtain the main property of these square matrices $\mathcal{MQ}_\nu$, $\mu_2 - 1 \leqslant \nu \leqslant d - 1$: their determinants are all equal to an implicit equation of the curve $\mathcal{C}$, raised to the power the degree of ϕ, as stated in Proposition 3.

In summary, the family of matrices $\mathcal{MQ}_\nu(\phi)$, $\nu \geqslant \mu_2 - 1$, gives implicit matrix representations of the rational curve $\mathcal{C}$. It is an extension of the family of matrices $\mathcal{M}_\nu(\phi)$, $\nu \geqslant d - 1$ with more compact matrices obtained by introducing moving conics. The more compact matrix, namely $\mathcal{MQ}_{\mu_2-1}$, is made of a Sylvester block built from the polynomial p_1, possibly empty if $\mu_1 = \mu_2$, and then filled by columns with Sylvester forms.

In the next section, we will generalize the above results to the case of rational curves in arbitrary dimension. The family of matrices $\mathcal{M}_\nu(\phi)$ built solely with moving lines, i.e. such that $\nu \geqslant d - 1$, has already been extended to this setting in [11]; we will review it briefly. The main contribution of this paper is the generalization of the matrices built with moving conics, i.e. the matrices $\mathcal{MQ}_\nu(\phi)$ such that $\mu_2 - 1 \leqslant \nu \leqslant d - 2$.

3. The method of moving quadrics

In what follows, we suppose that an homogeneous parameterization of a rational curve $\mathcal{C} \subset \mathbb{P}^n$, $n \geqslant 2$, is given over a field $\mathbb{K}$ by

$$\begin{array}{rccl} \phi: & \mathbb{P}^1 & \to \mathbb{P}^n & \\ & (s:t) & \mapsto (f_0(s,t) : f_1(s,t) : \cdots : f_n(s,t)), & \end{array} \tag{5}$$

where $f_0, \ldots, f_n$ are homogeneous polynomials in $\mathbb{K}[s, t]$ of the same degree $d \geqslant 1$. As in the case of plane curves, for the sake of simplicity we assume without loss of generality

that these polynomials have no common factor, so that the map ϕ is well defined everywhere on $\mathbb{P}^1$.

Unlike the case of plane curves, if $n \geqslant 3$ a single polynomial equation in $\mathbb{K}[x_0, \ldots, x_n]$ is not sufficient to describe implicitly the curve $\mathcal{C}$. Such an equation describe an hypersurface in $\mathbb{P}^n$ and hence a collection of at least $n-1$ of them are necessary for characterizing a curve by a dimension argument, and in general more than $n-1$ equations are needed. To be more precise, consider the ring morphism

$$\begin{array}{rcl} \mathbb{K}[x_0, \ldots, x_n] & \to & \mathbb{K}[s,t] \\ x_i & \mapsto & f_i(s,t),\ i = 0, \ldots, n. \end{array}$$

The set of polynomials that are in the kernel of this map, that is to say the polynomials $P(x_0, \ldots, x_n)$ such that $P(f_0, \ldots, f_n) = 0$, is an ideal of $\mathbb{K}[x_0, \ldots, x_n]$ that is called the defining ideal of the curve $\mathcal{C}$, denoted $\mathfrak{I}_{\mathcal{C}}$. Choosing a finite set of generators of this ideal with a good shape and in small number is known to be a difficult task (see for instance [21, 3, 9]). In what follows, an alternative implicit representation under the form of a matrix whose entries depend on the variables $x_0, \ldots, x_n$, is presented.

3.1. Moving hyperplanes and μ-basis

As a straightforward generalization of the concept of moving lines for planar curves, a *moving hyperplane* of degree $\nu \in \mathbb{N}$ is a polynomial of the form

$$H(s,t;x_0,\ldots,x_n) = g_0(s,t)x_0 + \cdots + g_n(s,t)x_n$$

where $g_0, \ldots, g_n$ are homogeneous polynomials in $\mathbb{K}[s,t]$ of degree ν. Thus, for any point $(s_0 : t_0) \in \mathbb{P}^1$, $H(s_0, t_0; x_0, \ldots, x_n)$ can be interpreted as the defining equation of a hyperplane in $\mathbb{P}^n$ that moves when the point $(s_0 : t_0)$ varies in $\mathbb{P}^1$. The moving hyperplane H is said to follow the parameterization ϕ if

$$H(s,t;f_0(s,t),\ldots,f_n(s,t)) = g_0 f_0 + \cdots + g_n f_n = 0,$$

which means geometrically that this hyperplane of equation $H = 0$ goes through the point $\phi(s:t) \in \mathcal{C}$.

For any integer ν, one can compute a basis $H_1, \ldots, H_{r_\nu}$ of the vector space (over $\mathbb{K}$) of the moving hyperplanes of degree ν following ϕ. Then, one can define a coefficient matrix $\mathbb{M}_\nu$ by means of the following equality:

$$\begin{pmatrix} s^\nu & s^{\nu-1}t & \cdots & t^\nu \end{pmatrix} \cdot \mathbb{M}_\nu = \begin{pmatrix} H_1 & \cdots & H_{r_\nu} \end{pmatrix}.$$

The matrix $\mathbb{M}_\nu$ is of size $(\nu+1) \times r_\nu$ and its entries are linear forms in $\mathbb{K}[x_0, \ldots, x_n]$, so it makes sense to evaluate it at a point in $\mathbb{P}^n$. For instance, by definition we have that for all point $(s_0 : t_0) \in \mathbb{P}^1$ this matrix satisfies to

$$\begin{pmatrix} s_0^\nu & s_0^{\nu-1}t_0 & \cdots & t_0^\nu \end{pmatrix} \cdot \mathbb{M}_\nu(\phi(s_0,t_0)) = \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix}. \quad (6)$$

This property implies that for any integer ν and any point $p \in \mathcal{C}$ the cokernel (or left nullspace) of $\mathbb{M}_\nu(p)$ has positive dimension. Actually, one can show that if $\nu \geqslant d-1$ then $r_\nu > \nu + 1$ and we have that

$$\operatorname{rank} \mathbb{M}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

However, this first generalization of Proposition 1 can be improved, but in order to state it we first need to introduce the concept of μ-basis for a parameterized curve in $\mathbb{P}^n$, $n \geqslant 2$, that has been introduced in [2] and then extensively studied (see e.g. [7] and [6, §4]).

Proposition 6. *There exist n moving hyperplanes $p_1, \ldots, p_n$ following ϕ such that any moving hyperplane H following ϕ can be written in the form*

$$H = h_1 p_1 + h_2 p_2 \ldots + h_n p_n,$$

where $h_1, \ldots, h_n$ are homogeneous polynomials in $\mathbb{K}[s,t]$. Such an n-tuple of moving hyperplanes $p_1, \cdots, p_n$ are called a μ-basis of the parameterization ϕ.

In addition, let $\mu_1, \ldots, \mu_n$ be the degrees of the polynomials $p_1, \ldots, p_n$ respectively and assume without loss of generality that $\mu_1 \leqslant \mu_2 \leqslant \ldots \leqslant \mu_n$. Then, the sequence $(\mu_1, \ldots, \mu_n)$ only depends on the parameterization ϕ and $\sum_{i=1}^n \mu_i = d$.

Proof. See e.g. [2, §5] and [7, §2]. □

Coming back to the family of matrices $\mathbb{M}_\nu$, they have a Sylvester block structure inherited from the existence of μ-basis. In particular,

$$r_\nu = \sum_{i=1}^{n} \max(0, \nu - \mu_i + 1). \quad (7)$$

Moreover, we have the following generalization of Proposition 1.

Proposition 7. *For all integer $\nu \geqslant \mu_n + \mu_{n-1} - 1$ we have $r_\nu > \nu + 1$ and*

$$\operatorname{rank} \mathbb{M}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

Proof. See [19]. □

As in the case of plane curves, the matrices $\mathbb{M}_\nu$ give implicit representations of the curve $\mathcal{C}$ for all ν above a certain threshold (observe that if $n = 2$ then $\mu_2 + \mu_1 - 1 = d - 1$). Indeed the point p on the curve $\mathcal{C}$ is characterized by the fact that the rank of such a matrix evaluated at p is not maximal. Compared to an implicit polynomial representation, this is much more efficient since only a single matrix is necessary. Moreover, these matrices allow to recover the pre-images of such points p and they are also adapted to numerical treatments by means of numerical linear algebra techniques (see [11, 12]). In what follows, we extend this family of matrices in order to obtain more compact matrices still providing an implicit representation of $\mathcal{C}$.

3.2. Moving quadrics

Not surprisingly, a *moving quadric* of degree $\nu \in \mathbb{N}$ is a polynomial of the form

$$Q(s,t;x_0,\ldots,x_n) = \sum_{0 \leq i \leqslant j \leq n} q_{ij}(s,t) x_i x_j$$

where $q_{i,j}(s,t)$, $0 \leq i \leqslant j \leq n$, are $n(n+1)/2$ homogeneous polynomials in $\mathbb{K}[s,t]$. In addition, a moving quadric is said to follow the parameterization ϕ if $Q(s,t;\phi(s,t)) = 0$, hence the polynomial Q defines a quadric in space that moves with the parameter $(s:t) \in \mathbb{P}^1$ and that goes through the point $\phi(s,t) \in \mathcal{C}$.

Choose an integer ν and let $\langle H_1, \ldots, H_{r_\nu} \rangle$ be a basis of the vector space of moving hyperplanes following ϕ. We can consider the vector space W_ν of moving quadrics following

ϕ. Each moving hyperplane H_j of degree ν following ϕ generates $n+1$ moving quadrics of the same degree ν, still following ϕ, that are given by $x_i H_j$, $0 \leq i \leq n$. Observe that geometrically, such a moving quadric consists of the union of the moving hyperplane of equation $H_j = 0$ and the static hyperplane of equation $x_i = 0$. We denote by V_ν the sub-vector space of moving quadrics generated by these moving quadrics obtained from moving hyperplanes. Now, let $\langle Q_1, \ldots, Q_{c_\nu} \rangle$ be basis of the quotient vector space W_ν / V_ν. Then, we define the matrix $\mathbb{MQ}_\nu(\phi)$ by

$$(H_1\ H_2\ \cdots\ H_{r_\nu}\ Q_1\ \cdots\ Q_{c_\nu}) = (s^\nu\ s^{\nu-1}t\ \cdots\ t^\nu) \cdot \mathbb{MQ}_\nu.$$

It is a matrix of size $(\nu+1) \times (r_\nu + c_\nu)$, r_ν being given by (7). Observe that this definition encapsulates the definition of the similar matrices we considered in the case $n = 2$. By definition, the first r_ν columns of $\mathbb{MQ}_\nu$ correspond to the matrix $\mathbb{M}_\nu$ introduced in §3.1 and its entries are linear forms in $\mathbb{K}[x_0, \ldots, x_n]$. On the other hand, its last c_ν columns are built from moving quadrics and hence its corresponding entries are quadratic forms in $\mathbb{K}[x_0, \ldots, x_n]$. The definition of the matrices $\mathbb{MQ}_\nu$ is translated into Algorithm 1.

Algorithm 1: Construction of the matrices $\mathbb{MQ}_\nu$

Input : A parameterization ϕ of a curve as defined in (5) and an integer ν.

Output: A matrix $\mathbb{MQ}_\nu$.

1. Compute a basis of the moving hyperplanes following ϕ of degree ν and build the matrix $\mathbb{M}_\nu$.
2. Compute a basis $\langle Q_1, \ldots, Q_{c_\nu} \rangle$ of the vector space $W_\nu \,/\, V_\nu$; its k-th element is of the form
$$Q_k = \sum_{0 \leqslant i \leqslant j \leqslant n} \sum_{l=0}^{\nu} c_{k,l,i,j} s^{\nu-l} t^l x_i x_j$$
3. Define the matrices $M_{i,j} = (c_{k,l,i,j})_{l,k}$ and the matrix $\mathbb{Q}_\nu = \sum_{0 \leqslant i \leqslant j \leqslant n} M_{i,j} x_i x_j$.
4. Return the concatenated matrix
$$\mathbb{MQ}_\nu = \left(\begin{array}{c|c} \mathbb{M}_\nu & \mathbb{Q}_\nu \end{array} \right).$$

We recall that the sequence of increasing integers $\mu_1 \leqslant \mu_2 \leqslant \ldots \leqslant \mu_n$ denote the degrees of a μ-basis of ϕ. Here is our first main result,

Theorem 8. *Assume that $\nu \geqslant \mu_n - 1$. Then $r_\nu + c_\nu \geqslant \nu + 1$ and*

$$\operatorname{rank} \mathbb{MQ}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

Moreover, we have that

$$c_\nu = \sum_{1 \leqslant i < j \leqslant n} \max(0, \mu_i + \mu_j - 1 - \nu).$$

In particular, if $\nu \geqslant \mu_n + \mu_{n-1} - 1$ then $c_\nu = 0$ and it follows that $\mathbb{MQ}_\nu = \mathbb{M}_\nu$.

The proof of this theorem is postponed to Section 3.4. For now, we discuss the shape of this matrix for some specific values of the degrees of the μ-basis. We emphasize that unlike in the case of plane curves, the matrices $\mathbb{MQ}_\nu$ will never be square matrices for space curves because a space curve cannot be defined by a single equation over an algebraically closed field.

In the family of matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_n - 1$, the matrix $\mathbb{MQ}_{\mu_n - 1}$ is evidently the one with the smallest number of rows. Moreover, the smallest possible value for the integer μ_n is $\lceil d/n \rceil$ because of the equality $\sum_{i=1}^n \mu_i = d$. It corresponds to the situation where the μ_i's are evenly distributed. It turns out that this balanced situation is the generic one when $\mathbb{K}$ is an algebraic closed field: fixing a degree d and picking n random homogeneous polynomials in (s,t) of degree d, $f_0, \ldots, f_n$ using a dense distribution of the coefficients such as Gaussian distribution, the degrees of its μ-basis are evenly distributed with probability 1 (see [22, Theorem 1.2] for the case $n = 2$ and [2, Section 3, Theorem 1] for a proof that generalizes to arbitrary dimension $n \geqslant 2$).

Here are some further specific settings:

- $\mu_1 = 0$: An element of degree 0 in the μ-basis corresponds to a (non-moving) hyperplane containing the curve. In this situation, we have $\mu_2 + \ldots + \mu_n = d$ and the problem is reduced to examining a curve in $\mathbb{P}^{n-1}$ whose a μ-basis is $(p_2, \ldots, p_n)$.
- $\mu_1 = \mu_2 = 1$: In this situation, the curve is contained in a (non-moving) quadric whose equation is given by the resultant of p_1 and p_2).
- $\mu_i = d/n$ for all i: In this case, the degree d is a multiple of n and the matrix $\mathbb{MQ}_{d/n-1}$ is purely quadratic since there is no moving hyperplane of degree $d/n - 1$ following the parameterization.

3.3. Sylvester forms

For any couple of integers $1 \leqslant i < j \leqslant n$ and any $\alpha = (\alpha_1, \alpha_2)$ such that $|\alpha| \leqslant \mu_i - 1$, one can consider the Sylvester form $\operatorname{syl}_\alpha(p_i, p_j)$, as defined in §2.4. Similarly to Lemma 4, one can show that it is a moving quadric following ϕ of degree $\mu_i + \mu_j - 2 - |\alpha|$ that is independent of the choice of decomposition modulo the polynomials p_i, p_j.

Now, for any integer ν consider the vector space S_ν that is generated by all the Sylvester forms of degree ν, i.e.

$$\mathrm{S}_\nu = \langle \operatorname{syl}_\alpha(p_i, p_j) \text{ such that } 1 \leq i < j \leq n \text{ and } |\alpha| = \mu_i + \mu_j - 2 - \nu \rangle.$$

Taking again the notation of §3.2, it is a sub-vector space of the space W_ν of moving quadrics of degree ν following ϕ. Here is our second main result.

Theorem 9. *If $\nu \geq \mu_n - 1$ then $W_\nu = V_\nu \oplus \mathrm{S}_\nu$. In other words, the moving quadrics of degree ν following ϕ are generated by the moving hyperplanes of degree ν following ϕ and by the Sylvester forms of degree ν. Moreover, these latter Sylvester forms are linearly independent and hence*

$$\dim \mathrm{S}_\nu = c_\nu = \sum_{1 \leqslant i < j \leqslant n} \max(0, \mu_i + \mu_j - \nu - 1).$$

The proof of this theorem is postponed to §3.4. Compared to Algorithm 1 described in §3.2, this theorem shows that the matrices $\mathbb{MQ}_\nu$ can be computed in *closed form* in terms of the polynomials $p_1, \ldots, p_n$ defining a μ-basis of ϕ. We

notice that, as far as we know, there is no known method that allows to compute the degrees $\mu_1, \dots, \mu_n$, or even the degree μ_n, efficiently without actually computing a μ-basis. So, assuming the a μ-basis is computed, Theorem 9 gives an optimal method to build an implicit matrix representation of the curve $\mathcal{C}$ since it shows that the matrices $\mathbb{MQ}_\nu$ can be computed essentially at the cost of computing a μ-basis. This is described with more details in Algorithm 2 for the smallest matrix $\mathbb{MQ}_{\mu_n-1}$. Of course, a similar algorithm can be used to build the matrix $\mathbb{MQ}_\nu$ for any integer $\nu \geqslant \mu_n - 1$, but we prefer to focus on the smallest matrix which is the more useful in practice.

Algorithm 2: Construction of $\mathbb{MQ}_{\mu_n-1}$

Input : A parametric curve ϕ defined by (5)
Output: The matrix $\mathbb{MQ}_{\mu_n-1}$.

1. Compute a μ-basis $(p_1, \dots, p_n)$ of ϕ. Let μ_i be the degree of p_i and assume that $\mu_1 \leqslant \cdots \leqslant \mu_n$.
2. Let $\mathcal{B}$ be a basis of the polynomial of degree $\mu_n - 1$, for instance
$$\mathcal{B} := \{s^{\mu_n-1}, s^{\mu_n-2}t, \dots, t^{\mu_n-1}\}.$$
3. Initialize the matrix $\mathbb{MQ}_{\mu_n-1}$ to the empty matrix. We build it by successively adding columns as follows.
4. For i from 1 to $n-1$ add a block of $\mu_n - \mu_i$ columns to the matrix $\mathbb{MQ}_{\mu_n-1}$ corresponding to the coefficients of the polynomials
$$\{s^{\mu_n-\mu_i-1}p_i, s^{\mu_n-\mu_i-2}tp_i, \dots, t^{\mu_n-\mu_i-1}p_i\}$$
with respect to the polynomial basis $\mathcal{B}$.
5. For i from 1 to $n-1$ do
for j from $i+1$ to n do
if $\nu_{i,j} := \mu_i + \mu_j - \mu_n - 1 \geqslant 0$ then add a block of $\nu_{i,j}+1$ columns to the matrix $\mathbb{MQ}_{\mu_n-1}$ corresponding to the coefficients of the Sylvester forms
$$\{\mathrm{syl}_\alpha(p_i, p_j) : |\alpha| = \nu_{i,j}\}$$
with respect to the polynomial basis $\mathcal{B}$.
6. Return the matrix $\mathbb{MQ}_{\mu_n-1}$.

3.4. Proofs of the main theorems

In the case of plane curves, the proofs of Proposition 3 and Proposition 5 can be done via an identification with the classical Sylvester and hybrid Bézout matrices, relying on their well-known properties. Indeed, it is a classical result that their determinants are all equal to the resultant of a μ-basis and that this latter is equal to an implicit equation of the parameterized curve $\mathcal{C}$ (raised to the power the degree of the corresponding parameterization). In the case of space curves, the situation is more complicated and much less classical for the simple reason that a polynomial implicit representation of the curve $\mathcal{C}$ requires several polynomial equations, a set of generators of the ideal $\mathfrak{I}_\mathcal{C}$. Thus, to prove Theorem 8 and Theorem 9 we need to use some more technical tools from algebraic geometry and commutative algebra, in our view inescapable.

Moving hypersurfaces We denote by I the ideal of the polynomial ring $R := \mathbb{K}[s,t;x_0,\dots,x_n]$ generated by all the moving planes following ϕ. It is hence generated by a μ-basis: $I = (p_1, \dots, p_n)$. Since we assumed that the defining polynomials $f_0, \dots, f_n$ of the parameterization ϕ have no common root in $\mathbb{P}^1$, we deduce that the polynomials $p_1, \dots, p_n$ have no common root in $\mathbb{P}^1$ as well [11, Lemma 1]. Algebraically, this means that they form a regular sequence [23, Chapter 17] in R outside $V(\mathfrak{m})$, the algebraic variety defined by the ideal $\mathfrak{m} := (s,t)$.

From the definitions we gave of moving hyperplanes and quadrics, it should be clear to the reader what we mean by a moving hypersurface. So, let J be the ideal of R generated by all the moving hypersurfaces, of any degree ν in (s,t) and any degree η in $x_0, \dots, x_n$, following ϕ. Since the μ-basis is a regular sequence outside $V(\mathfrak{m})$, then J is nothing but the saturation of I with respect to $\mathfrak{m}$, that is to say:
$$J = (I :_R \mathfrak{m}^\infty) = \{p \in R : \exists k \in \mathbb{N}\ p\mathfrak{m}^k \subset I\}. \tag{8}$$
The ideals I and J are both bi-graded ideals. They have a grading with respect to the variables s,t and with respect to the variables $x_0, \dots, x_n$. We denote by I_ν and J_ν the graded slices of degree $\nu \in \mathbb{N}$ with respect to the variables s,t. They are $\mathbb{K}[x_0,\dots,x_n]$-modules [23, §0.3]. For instance, $J_0 = J \cap \mathbb{K}[x_0,\dots,x_n] = \mathfrak{I}_\mathcal{C}$.

Elimination and matrices. We have previously built matrices by columns with the coefficients with respect to s,t of some moving hyperplanes and quadrics following ϕ of a given degree ν. Extending this approach, we could consider similar matrices built by columns with the coefficients of all the moving hypersurfaces following ϕ in a given degree ν. Call these matrices $\mathbb{MH}_\nu$. Their entries are homogeneous polynomials in $\mathbb{K}[x_0,\dots,x_n]$. They are defined up to a choice of basis of the polynomials in s,t of degree ν, and up to a choice of a set of generators of the set of moving hypersurfaces following ϕ of degree ν.

Lemma 10. *For any integer $\nu \geqslant 0$ and any $p \in \mathbb{P}^n$,*
$$\operatorname{rank} \mathbb{MH}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

Proof. Set $A := \mathbb{K}[x_0,\dots,x_n]$. Because of (8), we get that the annihilator $\operatorname{ann}_A(R_\nu/J_\nu)$ is equal to the defining ideal $\mathfrak{I}_\mathcal{C}$ of the curve $\mathcal{C}$ for all integer $\nu \geqslant 0$ [11, §2.3]. Then, by classical properties of Fitting ideals [23, Chapter 20], we obtain that any free presentation of R_ν/J_ν, as a A-module, has the claimed property. As J is generated by all the moving hypersurfaces following ϕ, the conclusion follows. □

Although interesting, this property is not of practical interest because it is a difficult task to compute moving hypersurfaces in general. For instance, the extreme case $\mathbb{MH}_0$ is a row matrix filled by columns with a generating set of $\mathfrak{I}_\mathcal{C}$. Nevertheless, with this interpretation, the main idea of the method of moving hyperplanes, resp. moving quadrics, is to tune the integer ν in order to have a control on the moving hypersurfaces that are needed. Typically, one may wonder for which integer ν the moving hyperplanes, resp. quadrics, generate all the moving hypersurfaces following ϕ in this degree. Thus, Proposition 7 means that
$$\forall \nu \geqslant \mu_n + \mu_{n-1} - 1 \quad J_\nu = I_\nu, \tag{9}$$
i.e. above this threshold degree all the moving hypersurfaces following ϕ are generated by the moving hyperplanes

of the same degree following ϕ. In the same vain, to prove Theorem 8, we have to show that

$$\forall \nu \geqslant \mu_n - 1 \quad J_\nu = (J\langle 2\rangle)_\nu \tag{10}$$

where $J\langle 2\rangle \subset J$ denotes the ideal of R generated by all the moving planes and moving quadrics following ϕ.

Local cohomology. A key ingredient in analyzing (9) and (10) is the local cohomology [23, Appendix 4] of the quotient ring $B := R/I$ with respect to the ideal $\mathfrak{m} = (s,t)$, denoted $H^i_{\mathfrak{m}}(B)$, $i \geqslant 0$. Indeed, by definition

$$H^0_{\mathfrak{m}}(B) = \{p \in B : \exists k \in \mathbb{N}\ p\mathfrak{m}^k = 0\} = (I :_B \mathfrak{m}^\infty)/I = J/I.$$

So, $H^0_{\mathfrak{m}}(B)$ is simply the quotient of the ideal of moving hypersurfaces following ϕ be the ideal of moving hyperplanes following ϕ. The other modules $H^i_{\mathfrak{m}}(B)$ are obtained as the cohomology of the Cech complex [23, Appendix 4]; it is of the form

$$\mathcal{C}^\bullet_{\mathfrak{m}}(B) : 0 \to B \to \oplus_{i=0}^n B_{x_i} \to \cdots \to B_{x_0\cdots x_n}$$

where the maps are localization maps with some carefully chosen signs. They inherit from B the two gradings with respect to s,t and $x_0,\ldots,x_n$. We recall that local cohomology commutes with direct sums of modules and that the local cohomology of the polynomial ring $R = A \otimes_{\mathbb{K}} \mathbb{K}[s,t]$ with respect to $\mathfrak{m}$ is well known: $H^i_{\mathfrak{m}}(R) = 0$ if $i \neq 2$ and

$$H^2_{\mathfrak{m}}(R) \simeq A \otimes_{\mathbb{K}} \check{S},\ \check{S} := \frac{1}{st}\mathbb{K}[s^{-1},t^{-1}]. \tag{11}$$

For instance, we deduce that $H^2_{\mathfrak{m}}(R)_\nu = 0$ for all $\nu > -2$.

The Koszul complex. Another key ingredient to deal with the properties (9) and (10) is the Koszul complex [23, Chapter 17]. We consider the Koszul complex associated to sequence $p_1,\ldots,p_n$ that generates the ideal I. We will need to examine both gradings with respect to $\mathbb{K}[s,t]$ and to $\mathbb{K}[x_0,\ldots,x_n]$: we denote the shifts in degrees by $[-]$, resp. $\{-\}$, with respect to $\mathbb{K}[s,t]$, resp. $\mathbb{K}[x_0,\ldots,x_n]$. With this notation, this Koszul complex is of the form

$$K_\bullet : K_n \xrightarrow{d_n} \cdots \to K_2 \xrightarrow{d_2} K_1 \xrightarrow{d_1} K_0 = R$$

where $K_1 = \oplus_{i=1}^n R[-\mu_i]\{-1\}$ and $K_p = \wedge^p K_1$, the map d_1 being given by the row matrix filled with the p_i's. It is immediate to see that $H_0(K_\bullet) = R/I = B$.

Proposition 11. *With the above notation, we have an isomorphism of graded modules*

$$H_2(H^2_{\mathfrak{m}}(K_\bullet)) \xrightarrow{\sim} H^0_{\mathfrak{m}}(B) = J/I.$$

Proof. This proof uses spectral sequences [23, A.3.13]. Consider the double complex $\mathcal{C}^\bullet_{\mathfrak{m}}(K_\bullet)$ obtained from the Koszul complex $K_\bullet$ by extending each term K_p with its corresponding Cech complex $\mathcal{C}^\bullet_{\mathfrak{m}}(K_p)$. The spectral sequence corresponding to the column filtration of our double complex converges at the second step because the polynomials $p_1,\ldots,p_n$ form a regular sequence outside $V(\mathfrak{m})$. Therefore, we obtain the following terms

$$\begin{array}{ccccc} H^0_{\mathfrak{m}}(H_n(K_\bullet)) & \cdots & H^0_{\mathfrak{m}}(H_1(K_\bullet)) & H^0_{\mathfrak{m}}(H_0(K_\bullet)) \\ 0 & \cdots & 0 & H^1_{\mathfrak{m}}(H_0(K_\bullet)) \\ 0 & \cdots & 0 & 0. \end{array}$$

On the other hand, the row filtration of our double complex gives another spectral sequence that also converge at the second step; we get:

$$\begin{array}{ccccc} 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \\ H_n(H^2_{\mathfrak{m}}(K_\bullet)) & \cdots & H_1(H^2_{\mathfrak{m}}(K_\bullet)) & H_0(H^2_{\mathfrak{m}}(K_\bullet)) \end{array}$$

From here, since $H_0(K_\bullet) = B$, the claimed isomorphism follows from the fact that these two spectral sequences converge to the same limit, namely the homology of the total complex of $\mathcal{C}^\bullet_{\mathfrak{m}}(K_\bullet)$. □

Corollary 12. *Assume that $\nu \geqslant \mu_n - 1$, then we have the following exact sequence of graded A-modules*

$$\bigoplus_{1\leqslant i<j<k\leqslant n} \check{S}_{\nu-\mu_i-\mu_j-\mu_k} \otimes_{\mathbb{K}} A\{-3\} \to \bigoplus_{1\leqslant i<j\leqslant n} \check{S}_{\nu-\mu_i-\mu_j} \otimes_{\mathbb{K}} A\{-2\} \to (J/I)_\nu \to 0.$$

Proof. The homology module $H_2(H^2_{\mathfrak{m}}(K_\bullet))$ is computed as follows. First, applying the functor $H^2_{\mathfrak{m}}(-)$ to the Koszul complex $K_\bullet$ we get the sequence

$$H^2_{\mathfrak{m}}(K_3) \xrightarrow{d_3} H^2_{\mathfrak{m}}(K_2) \xrightarrow{d_2} H^2_{\mathfrak{m}}(K_1) \tag{12}$$

where the maps are induced by those of the Koszul complex $K_\bullet$. Then, $H_2(H^2_{\mathfrak{m}}(K_\bullet))$ is simply $\ker d_2/\operatorname{Im} d_3$. Now, since $K_1 = \oplus_{i=1}^n R[-\mu_i]\{-1\}$, by (11) we deduce that

$$H^2_{\mathfrak{m}}(K_1)_\nu \simeq \oplus_{i=1}^n \check{S}_{\nu-\mu_i} \otimes_{\mathbb{K}} A\{-1\}.$$

In particular, we deduce that for all $\nu > \mu_n - 2$, $H^2_{\mathfrak{m}}(K_1)_\nu = 0$. Therefore, we deduce that $(\ker d_2)_\nu = H^2_{\mathfrak{m}}(K_2)_\nu$. From here, the claimed result follows by noting that

$$K_2 = \oplus_{1\leqslant i<j\leqslant n} R[-\mu_i-\mu_j]\{-2\},$$

$$K_3 = \oplus_{1\leqslant i<j<k\leqslant n} R[-\mu_i-\mu_j-\mu_k]\{-3\},$$

and applying again (11). □

Theorem 8 follows straightforwardly from this corollary. Indeed, it shows that J_ν is generated by moving quadrics modulo the moving planes, i.e. modulo I_ν, and that the number of minimal generators is precisely given by c_ν. In particular, if $\nu \geqslant \mu_n + \mu_{n-1} - 1$ we get that $(J/I)_\nu = 0$, i.e. that $J_\nu = I_\nu$.

Duality and Sylvester forms. The proof of Theorem 9 can be seen as a particular case of an explicit construction of duality isomorphism similar to the one we obtained in Proposition 11. Such an explicit construction already appeared in [24] and [25]. It is beyond the scope of this paper to give all the details about this construction, but we mention the main steps to prove Theorem 9.

First, by Koszul self-duality [23, Proposition 17.15], we have a graded isomorphism

$$H_2(H^2_{\mathfrak{m}}(K_\bullet)) \simeq H_{n-2}(K_\bullet[d-2])^*$$

where $(-)^*$ stands for the dual. Then, one can consider the generalized Morley form that appears in [24, Section 3] and that gives an explicit construction of the map in Proposition

11, via the above isomorphism. Then, to obtain Theorem 9 one has to show that for all degree $\nu \geqslant \mu_n - 1$ the graded components of this Morley form coincide with Sylvester forms. This latter property follows from [18, Proposition 3.11.13] (see also [19, Lemma 2.8]).

The Koszul syzygies. Before closing this section, we discuss the link with the obvious moving hyperplanes of the form (3) that are also called Koszul syzygies. Let us denote by $I_{\mathcal{K}}$ the ideal generated by these moving hyperplanes. We have $I_{\mathcal{K}} \subset I \subset J$. As the polynomials $f_0, \ldots, f_n$ have no common root in $\mathbb{P}^1$, we know that these three ideals coincide in sufficiently high degrees. Here is a more precise result.

Proposition 13. *For all $\nu \geqslant d + \mu_n + \mu_{n-1} - 1$ we have $(I_{\mathcal{K}})_\nu = I_\nu$.*

Proof. The quotient $I/I_{\mathcal{K}}$ is canonically identified with the first homology group H_1^f of the Koszul complex associated to the sequence $f_0, \ldots, f_n$ which is of the form

$$K_{n+1}^f \to \cdots \to K_2^f \xrightarrow{d_2} K_1^f \xrightarrow{d_1} K_0^f.$$

Indeed, the kernel of d_1 corresponds to the moving planes following ϕ and the image of d_2 identifies to the obvious moving hyperplanes. Taking into account the shifts in the grading, we get the isomorphism $(H_1^f)_{\nu+d} \simeq (I/I_{\mathcal{K}})_\nu$ for all integer ν.

Now, consider the sequence

$$0 \to Z_2^f \hookrightarrow K_2^f \xrightarrow{d_2} K_1^f \xrightarrow{d_1} K_0^f$$

where $Z_2^f = \ker d_2$. Then, playing as in the proof of Proposition 11 with the two spectral sequences associated to the double complex

$$0 \to \mathcal{C}_{\mathfrak{m}}^\bullet(Z_2^f) \hookrightarrow \mathcal{C}_{\mathfrak{m}}^\bullet(K_2^f) \xrightarrow{d_2} \mathcal{C}_{\mathfrak{m}}^\bullet(K_1^f) \xrightarrow{d_1} \mathcal{C}_{\mathfrak{m}}^\bullet(K_0^f),$$

we deduce that $(H_1^f)_\nu = 0$ for any integer ν such that $H^2_{\mathfrak{m}}(Z_2^f)_\nu = 0$.

The two modules Z_2^f and Z_1^f are free graded $\mathbb{K}[s,t]$-modules. Consider the canonical map $\wedge^2 Z_1^f \to Z_2^f$. Since the f_i's have no common root in $\mathbb{P}^1$, we deduce that the kernel and the cokernel of this map are supported on $V(\mathfrak{m})$, and therefore it must be an isomorphism, moreover graded. To conclude, we notice that $Z_1^f \simeq \oplus_{i=1}^n \mathbb{K}[s,t](-d-\mu_i)$, and the claimed result follows by (11). □

3.5. Summary of our results

To summarize, we have built a family of matrices $\mathbb{MQ}_\nu$ that provides implicit matrix representations of a parameterized curve in arbitrary dimension for all $\nu \geqslant \mu_n - 1$, where μ_n is the highest degree of a polynomial in a μ-basis of the parameterization of this curve. They have the following shape:

- If $\mu_n - 1 \leqslant \nu \leqslant \mu_n + \mu_{n-1} - 2$, then $\mathbb{MQ}_\nu$ is filled with moving planes and moving quadrics. It is exclusively filled with moving quadrics if and only if $\nu = \mu_n - 1$ and $\mu_i = d/n$ for all $i = 1, \ldots, n$.
- If $\nu \geqslant \mu_n + \mu_{n-1} - 1$, then $\mathbb{MQ}_\nu$ is filled with moving planes, and it coincides with the family of matrices $\mathbb{M}_\nu$ introduced in [11].
- If $\nu \geqslant d + \mu_n + \mu_{n-1} - 1$, then $\mathbb{MQ}_\nu = \mathbb{M}_\nu$ can be filled from the obvious moving planes of the form (3) without relying on the computation of a μ-basis. This is an improvement of [11, Proposition 26].

Example 1. *Consider the following parameterization ϕ of a curve $\mathcal{C}$ of degree 6:*

$$\begin{aligned}
f_0(s,t) &= 3s^4t^2 - 9s^3t^3 - 3s^2t^4 + 12st^5 + 6t^6,\\
f_1(s,t) &= -3s^6 + 18s^5t - 27s^4t^2 - 12s^3t^3 + 33s^2t^4 + 6st^5 - 6t^6,\\
f_2(s,t) &= s^6 - 6s^5t + 13s^4t^2 - 16s^3t^3 + 9s^2t^4 + 14st^5 - 6t^6,\\
f_3(s,t) &= -2s^4t^2 + 8s^3t^3 - 14s^2t^4 + 20st^5 - 6t^6.
\end{aligned}$$

The computation of a μ-basis of ϕ gives

$$\begin{aligned}
p_1 &= (s^2 - 3st + t^2)x + t^2y\\
p_2 &= (s^2 - st + 3t^2)y + (3s^2 - 3st - 3t^2)z,\\
p_3 &= 2t^2z + (s^2 - 2st - 2t^2)w,
\end{aligned}$$

so that we have $\mu_1 = \mu_2 = \mu_3 = 2$.

This example is taken taken from [9, Example 3.7] where the authors introduce three quartic surfaces in order to get an implicit representation of the curve $\mathcal{C}$. The equations of these quartic surfaces are given by the resultant of p_1 and p_2, of p_1 and p_3, and of p_2 and p_3 with respect to the homogeneous variables s and t. Their intersection always contains the curve $\mathcal{C}$ but it may also contains some extraneous components. For instance, in this example the point $q = (1:1:1:1) \in \mathbb{P}^3$ is not on the curve $\mathcal{C}$, but it belongs to the intersection of these three quartic surfaces.

In [11, Example 8], this same parameterization is implicitized by means of the matrix of moving hyperplanes $\mathbb{M}_3$ ($\mu_2 + \mu_3 - 1 = 3$), which is of size 4×6. This matrix is proved to always give an implicit representation of the curve $\mathcal{C}$. Indeed, its rank is equal to 4 after evaluation at the point q, showing that $q \notin \mathcal{C}$.

Now, according to the new family of matrices we built in this paper, the matrix of $\mathbb{MQ}_1$ ($\mu_3 - 1 = 1$) also provides an implicit representation of the curve $\mathcal{C}$. It is a matrix of size 2×6, more compact than $\mathbb{M}_3$, which is filled with the 6 Sylvester forms $\mathrm{syl}_{(1,0)}(p_i, p_j)$ and $\mathrm{syl}_{(0,1)}(p_i, p_j)$ for $1 \leqslant i < j \leqslant 3$. It is printed in Figure 1.

4. Computational aspects

In this section, we report on some experiments on the computation of the family of matrices $\mathbb{MQ}_\nu$ we have introduced. In particular, we illustrate the gain we obtain with the smallest matrix $\mathbb{MQ}_{\mu_n - 1}$ for deciding if a point belongs to a parameterized curve.

We emphasize that all the applications that are discussed in [11] with the matrices of moving hyperplanes also apply with our extended family of matrices built with moving hyperplanes and moving quadrics. For instance, the curve/curve intersection problem and the computation of the self-intersection locus of a parameterized curve can be solved with these new matrices following essentially the same algorithms; we refer the reader to [11] for more details.

$$\begin{pmatrix} 2xy - y^2 - 6xz - 3yz & 2xy + 6xz & 2xz - 3xw - yw & xw & 2yz + 6z^2 - 5yw - 3zw & -yw - 3zw \\ -8xy + y^2 + 12xz + 3yz & 2xy - y^2 - 6xz - 3yz & -6xz + 8xw + 2yw & 2xz - 3xw - yw & -2yz - 6z^2 + 8yw & 2yz + 6z^2 - 5yw - 3zw \end{pmatrix}$$

FIGURE 1. matrix $\mathbb{MQ}_1$ of moving quadrics corresponding to the space curve parameterization discussed in Example 1.

4.1. Computation of μ-basis

To take the best advantage of the family of matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_n - 1$, it is necessary to compute a μ-basis of the input parameterized curve. Actually, we could argue that computing only the highest degree μ_n of a μ-basis would be enough for us, but as far as we know, there is no known method that allows to compute μ_n without computing an entire μ-basis. For the sake of completeness, we recall very briefly, and give references, for the three known types of methods for computing a μ-basis (see also [6]).

The first dedicated algorithm for computing a μ-basis appeared in [14, Algorithm 3.2], in the case of plane curves. Later, it has been generalized to the case of space curves in arbitrary dimension in [7, §3]. The method consists in considering the obvious moving hyperplanes (3) (or Koszul syzygies) and then to apply Gaussian elimination techniques in order to iteratively reduce these moving hyperplanes to a μ-basis.

Another approach for computing μ-bases comes from the methods and algorithms that are independently developed in order to compute canonical forms of univariate polynomial matrices. Thus, a μ-basis can be efficiently computed as a Popov form of a matrix built again from the obvious moving hyperplanes (3). As far as we know, the best complexity algorithm is described in [17]; for further details about Popov forms, we refer the reader to [26, 27].

Finally, we mention that a third approach for computing μ-bases has been recently given in [15]. It also relies on matrix reductions, but here a finer (partial) reduced row-echelon form is used.

4.2. Computation of the matrices

In this paragraph we report on the size and the computation time of some implicit matrix representations that are of particular interest, in the case $n = 3$. More precisely, we retain the following matrices:

- $\mathbb{M}$: a moving hyperplane matrix. It is considered either in degree $d-1$, in order to avoid the computation of a μ-basis, or in its optimal degree $\mu_n + \mu_{n-1} - 1$, in which case (the degrees of) a μ-basis must be computed.
- $\mathbb{MQ}_{\text{ker}}$: the matrix of moving planes and moving quadrics in degree $\mu_n - 1$, computed using kernel calculations by Algorithm 1.
- $\mathbb{MQ}_{\text{Syl}}$: the matrix of moving planes and moving quadrics in degree $\mu_n - 1$ built in closed form from a μ-basis, by means of Algorithm 2.

The results are reported below. The algorithms have been implemented in SageMath and run using an Intel(R) Pentium(R) N3540 CPU @ 2.16GHz on a x64 machine with 4GB of RAM.

In Table 1, we give the computation time of a μ-basis and then our two options to build an optimal implicit matrix representation: a matrix fully composed of moving planes or a mixed matrix with moving planes and moving quadrics. For these two matrices, the computation time excludes the computation of the μ-basis, which is reported in the second column. It appears clearly that the matrix with moving quadrics is more expensive to build, because its entries require calculations.

Degree d and degrees $(\mu_i)_i$	**μ-basis**	$\mathbb{M}_{\boldsymbol{\mu_n+\mu_{n-1}-1}}$	$\mathbb{MQ}_{\mathbf{Syl},\boldsymbol{\mu_n-1}}$
5 (2, 3)	230ms	5x5 57ms	3x3 417ms
10 (5, 5)	343ms	10x10 168ms	5x5 1503ms
10 (1, 9)	292ms	10x10 166ms	9x9 614ms
5 (1, 2, 2)	156ms	4x7 94ms	2x5 676ms
9 (3, 3, 3)	151ms	6x9 141ms	3x9 2194ms
9 (1, 4, 4)	292ms	8x15 268ms	4x9 1900ms
9 (1, 1, 7)	396ms	8x15 244ms	7x14 1132ms
15 (5, 5, 5)	281ms	10x15 332ms	5x15 5516ms
15 (1, 7, 7)	647ms	14x27 782ms	7x15 4663ms
15 (1, 1, 13)	1477ms	14x27 657ms	13x26 2810ms

Table 1: Computation time in milliseconds of a μ-basis and two typical implicit matrix representations built from the μ-basis.

In the Table 2, we assume that a μ-basis is unknown and then compare the computation time of the matrix $\mathbb{M}_{d-1}$, which does not require the computation of a μ-basis, with the computation time of the matrix $\mathbb{MQ}_{\mu_n-1}$ via our two algorithms, for which a μ-basis is computed. As expected, the faster matrix to compute is $\mathbb{M}_{d-1}$.

Degree d and degrees $(\mu_i)_i$	$\mathbb{M}_{\boldsymbol{d-1}}$	$\mathbb{MQ}_{\mathbf{ker},\boldsymbol{\mu_n-1}}$	$\mathbb{MQ}_{\mathbf{Syl},\boldsymbol{\mu_n-1}}$
5 (2, 3)	74ms	305ms	431ms
10 (5, 5)	226ms	409ms	1113ms
10 (1, 9)	187ms	1055ms	614ms
5 (1, 2, 2)	120ms	319ms	663ms
9 (3, 3, 3)	312ms	458ms	1914ms
9 (1, 4, 4)	384ms	987ms	1912ms
9 (1, 1, 7)	304ms	2815ms	1150ms
15 (5, 5, 5)	931ms	1358ms	5989ms
15 (1, 7, 7)	701ms	2311ms	4363ms
15 (1, 1, 13)	946ms	8947ms	2526ms

Table 2: Comparison of the computation time to build the matrix $\mathbb{M}_{d-1}$ with the computation times of the two algorithms corresponding to build the moving quadric matrices either from kernel computation or by instantiation of Sylvester forms.

In summary, it appears that the new matrix $\mathbb{MQ}_{\mu_n-1}$ is not easier to build compared to the other matrices that are already known, but their computation time remains acceptable. It turns out that these implicit matrix representations

are only computed once for a curve and is then stored. So in the end, the computation of the matrix itself is not the most important feature, what is the most important is the efficiency of a matrix when one computes intensively on the curve with it. In the next paragraph, we illustrate this property with the point/curve intersection problem, i.e. by testing whether a given point belongs to the curve. As we will see, for this use the matrices of moving quadrics we introduce behave much better than the previously known matrices.

4.3. The drop-of-rank property

What makes the matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_n - 1$, implicit representations is the *drop-of-rank property*: evaluated at a point p, their rank drops, more precisely their rows are linearly dependent, if and only if the point p is on the curve. This property gives a very efficient method to decide if a point belongs to a curve or not.

In Table 3, we compare the computation time for testing if a point belongs to a curve by means of the two moving hyperplanes matrices, $\mathbb{M}_{d-1}$ which is computed without μ-basis and $\mathbb{M}_{\mu_n+\mu_{n-1}-1}$ that requires the computation of a μ-basis, and by means of the smallest matrix of moving hyperplanes and quadrics we obtained, namely $\mathbb{MQ}_{\mu_n-1}$. In all cases we tested, whatever the repartition of the degrees μ_i of the μ-basis, this matrix $\mathbb{MQ}_{\mu_n-1}$ was always more efficient.

Degree d and degrees $(\mu_i)_i$	$\mathbb{M}_{\boldsymbol{d-1}}$	$\mathbb{M}_{\boldsymbol{\mu_n+\mu_{n-1}-1}}$	$\mathbb{MQ}_{\boldsymbol{\mu_n-1}}$
5 (2, 3)	54ms	54ms	22ms
10 (5, 5)	230ms	230ms	62ms
10 (1, 9)	230ms	230ms	121ms
5 (1, 2, 2)	105ms	61ms	22ms
9 (3, 3, 3)	353ms	125ms	59ms
9 (1, 4, 4)	393ms	267ms	78ms
9 (1, 1, 7)	362ms	256ms	171ms
15 (5, 5, 5)	1139ms	377ms	167ms
15 (1, 7, 7)	1127ms	929ms	199ms
15 (1, 1, 13)	1086ms	894ms	534ms

Table 3: Average time over a hundred random points for testing if a point belongs to the curve.

We notice that deciding whether a point in space belongs to a parameterized curve can be done via a greatest common divisor (GCD) computation once a μ-basis is known. Indeed, let p_1, p_2, p_3 be a μ-basis of a curve parameterization, let q be a point in space and denote by $p_i(q)$ the evaluation of p_i at the point q. Then, the GCD of the three homogeneous polynomials $p_1(q)$, $p_2(q)$ and $p_3(q)$ is a homogeneous polynomial in the variables s, t whose degree is equal to the multiplicity of the point q with respect to the curve, in particular this degree is nonzero if and only if the point q belongs to the curve [28, Theorem 6.4]. However, this method requires exact computations and hence it does not allow to deal with approximate input data. In addition, the use of exact computations makes the computation time strongly dependent on the choice of the point q. To be more concrete, we applied this method to the case of the degree 9 curve with μ-basis of type $(3, 3, 3)$ that is used in Table 3. The points are chosen on the curve with five significant digits and are cast to rational numbers for the GCD computation. We observed an average time over a hundred random points of 66 121ms and especially a very high standard deviation of 66 593ms (with a minimum of 15ms and a maximum computation time of 176 136ms). When the matrix $\mathbb{MQ}_2$ is used we observe a standard deviation of 7ms, showing a computation time which is almost independent of the point q. This difference is mostly due to the fact that the matrices of moving hyperplanes and moving quadrics allow to rely on numerical linear algebra tools and are thus capable to deal with approximate data and computations.

To conclude, we illustrate that given a point $p \in \mathcal{C}$, not only the rank of $\mathbb{MQ}_\nu(p)$, $\nu \geqslant \mu_n - 1$, drops but also its cokernel (left nullspace) allows to recover all the parameters $(s_0 : t_0) \in \mathbb{P}^1$ such that $\phi(s_0, t_0) = p$, following the approach developed in [11, 12] with the matrices of moving hyperplanes.

Example 2. *Consider the lemniscate-like space curve $\mathcal{C}$ given by*

$$\begin{aligned} f_0(s,t) &= (t^2+s^2)(t^4+s^2),\\ f_1(s,t) &= t(t^2-s^2)^2,\\ f_2(s,t) &= t(t^4-s^4),\\ f_3(s,t) &= 3s^4+t^4. \end{aligned}$$

This curve has a self-intersection point at $p := (1 : 0 : 0 : 1)$. The matrix of moving quadrics $\mathbb{MQ}_2$ is of size 3×6 and, when evaluated at p, has a cokernel given by

$$v_1 = (v_{1,1}, v_{1,2}, v_{1,3}) = (1, 0, 1)$$

and

$$v_2 = (v_{2,1}, v_{2,2}, v_{2,3}) = (0, 1, 0).$$

None of these vectors are of the form $v = (s^2, st, t^2)$ but they are linear combinations of the two vectors corresponding to the evaluation of the form v at the two pre-images parameters of p. Therefore, to retrieve these two pre-images one can solve the eigenvalue problem

$$\operatorname{rank}(t\Delta_0 - s\Delta_1) < 2$$

where

$$\Delta_0 = \begin{pmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{pmatrix}, \quad \Delta_1 = \begin{pmatrix} v_{1,2} & v_{1,3} \\ v_{2,2} & v_{2,3} \end{pmatrix}.$$

We deduce that the pre-images of p correspond to the parameters $(s_0 : t_0) = (1 : 1)$ and $(s_1 : t_1) = (1 : -1)$.

Finally, we notice that the matrix $\mathbb{MQ}_1$ is of size 2×6 and satisfies to the drop-of-rank property. Its rank drops by 2 after evaluation at p, thus it is equal to the null matrix when evaluated at p. Therefore, in this case the matrix is too small to allow the inversion of a multiple point and hence it is necessary to increase the degree ν by one. In general a matrix $\mathbb{MQ}_\nu$ allows to invert points having at most ν pre-images.

5. Conclusion

The method of moving conics of Serdeberg et al. [3] is a very efficient method for solving the implicitization problem for plane parameterized curves. In this paper, we extended this method to rational space curves in arbitrary dimension.

The size of the smallest matrix we got is correlated to the degrees of a μ-basis of the curve. In addition, by using Sylvester forms we proved that this matrix is a generalized hybrid Bézout matrix, in the sense that it has a structure very similar to the one of the hybrid Bézout matrix of a μ-basis of a plane curve. Finally, the usefulness of these new matrices was illustrated for computing intensively on the curve, more precisely for deciding among many points which of them belong to a given rational curve.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675789.

References

References

[1] T. Sederberg, F. Chen, Implicitization using moving curves and surfaces, in: Proceedings of SIGGRAPH, Vol. 29, 1995, pp. 301–308. doi:10.1145/218380.218460.

[2] D. Cox, T. Sederberg, F. Chen, The moving line ideal basis of planar rational curves, Computer Aided Geometric Design 15 (8) (1998) 803 – 827. doi:10.1016/S0167-8396(98)00014-4.

[3] T. Sederberg, R. Goldman, H. Du, Implicitizing rational curves by the method of moving algebraic curves, J. Symbolic Comput. 23 (2-3) (1997) 153–175. doi:10.1006/jsco.1996.0081.

[4] D. Cox, R. Goldman, M. Zhang, On the validity of implicitization by moving quadrics of rational surfaces with no base points, J. Symbolic Comput. 29 (3) (2000) 419–440. doi:10.1006/jsco.1999.0325.

[5] Y. Lai, F. Chen, Implicitizing rational surfaces using moving quadrics constructed from moving planes, J. Symbolic Comput. 77 (2016) 127–161. doi:10.1016/j.jsc.2016.02.001.

[6] X. Jia, X. Shi, F. Chen, Survey on the theory and applications of μ-bases for rational curves and surfaces, journal of Computational and Applied Mathematics 329 (2018) 2 – 23, the International Conference on Information and Computational Science, 2–6 August 2016, Dalian, China. doi:10.1016/j.cam.2017.07.023.

[7] N. Song, R. Goldman, μ-bases for polynomial systems in one variable, Computer Aided Geometric Design 26 (2) (2009) 217 – 230. doi:10.1016/j.cagd.2008.04.001.

[8] J. Hoffman, H. Wang, X. Jia, R. Goldman, Minimal generators for the Rees algebra of rational space curves of type (1,1,d-2), Eur. J. Pure Appl. Math. 3 (4) (2010) 602–632.

[9] X. Jia, H. Wang, R. Goldman, Set-theoretic generators of rational space curves, J. Symbolic Comput. 45 (4) (2010) 414–433. doi:10.1016/j.jsc.2009.11.001.

[10] A. Kustin, C. Polini, B. Ulrich, Rational normal scrolls and the defining equations of Rees algebras, J. Reine Angew. Math. 650 (2011) 23–65. doi:10.1515/CRELLE.2011.002.

[11] L. Busé, T. Luu Ba, Matrix-based implicit representations of rational algebraic curves and applications, Computer Aided Geometric Design 27 (9) (2010) 681–699. doi:10.1016/j.cagd.2010.09.006.

[12] L. Busé, Implicit matrix representations of rational Bézier curves and surfaces, Computer-Aided Design 46 (2014) 14–24. doi:10.1016/j.cad.2013.08.014.

[13] L. Busé, M. Chardin, Implicitizing rational hypersurfaces using approximation complexes, J. Symbolic Comput. 40 (4-5) (2005) 1150–1168. doi:10.1016/j.jsc.2004.04.005.

[14] F. Chen, W. Wang, The μ-basis of a planar rational curve - properties and computation, Graphical Models 64 (2003) 368–381. doi:10.1016/S1077-3169(02)00017-5.

[15] H. Hong, Z. Hough, K. I., Algorithm for computing μ-bases of univariate polynomials, journal of Symbolic Computation 80 (2017) 844 – 874. doi:10.1016/j.jsc.2016.08.013.

[16] V. Neiger, V. Xuan, Computing canonical bases of modules of univariate relations, in: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '17, ACM, New York, NY, USA, 2017, pp. 357–364. doi:10.1145/3087604.3087656.

[17] W. Zhou, G. Labahn, A. Storjohann, Computing minimal nullspace bases, in: Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ISSAC '12, ACM, New York, NY, USA, 2012, pp. 366–373. doi:10.1145/2442829.2442881.

[18] J.-P. Jouanolou, Formes d'inertie et résultant: un formulaire, Advances in Mathematics 126 (2) (1997) 119 – 250. doi:10.1006/aima.1996.1609.

[19] L. Busé, T. Luu Ba, Matrix-based implicit representations of rational algebraic curves and applications, Computer Aided Geometric Design 27 (9) (2010) 681 – 699. doi:10.1016/j.cagd.2010.09.006.

[20] G. M. Diaz-Toca, L. Gonzalez-Vega, Barnett's theorems about the greatest common divisor of several univariate polynomials through Bézout-like matrices, J. Symbolic Comput. 34 (1) (2002) 59–81. doi:10.1006/jsco.2002.0542.

[21] E. Fortuna, P. Gianni, B. Trager, Generators of the ideal of an algebraic space curve, J. Symbolic Comput. 44 (9) (2009) 1234–1254. doi:10.1016/j.jsc.2008.02.014.

[22] C. D'Andrea, On the structure of μ-classes, Communications in Algebra 32 (2004) 159–165. doi:10.1081/AGB-120027858.

[23] D. Eisenbud, Commutative algebra, Vol. 150 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1995, with a view toward algebraic geometry.

[24] J.-P. Jouanolou, An explicit duality for quasi-homogeneous ideals, J. Symbolic Comput. 44 (7) (2009) 864–871. doi:10.1016/j.jsc.2008.04.011.

[25] D. A. Cox, Bezoutians and Tate resolutions, J. Algebra 311 (2) (2007) 606–618. doi:10.1016/j.jalgebra.2006.11.029.

[26] G. Villard, Computing popov and hermite forms of polynomial matrices, in: Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, ISSAC '96, ACM, New York, NY, USA, 1996, pp. 250–258. doi:10.1145/236869.237082.

[27] T. Mulders, A. Storjohann, On lattice reduction for polynomial matrices, journal of Symbolic Computation 35 (4) (2003) 377 – 401. doi:10.1016/S0747-7171(02)00139-6.

[28] H. Wang, X. Jia, R. Goldman, Axial moving planes and singularities of rational space curves, Computer Aided Geometric Design 26 (3) (2009) 300 – 316. doi:https://doi.org/10.1016/j.cagd.2008.09.002.